ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 3, March 2017

A Survey on Database Requirements and Security of IoT

Bhamiti Joshi [1], Shreya Khobragade [2], K.K. Joshi [3]

M.Tech. Student, Department of Computer Engineering & Information Technology, Veermata Jijabai Technological Institute, Mumbai, Maharashtra, India [1]

M.Tech. Student, Department of Computer Engineering & Information Technology, Veermata Jijabai Technological Institute, Mumbai, Maharashtra, India [2]

Assistant Professor, Department of Computer Engineering & Information Technology, Veermata Jijabai Technological Institute, Mumbai, Maharashtra, India [3]

ABSTRACT: The Internet Of Things (IOT) has emerged as a trustworthy technology to improve the quality of life through offering various automated, interactive and comfortable services. Sensors are integrated at different places in homes, offices and in clothes also, equipment and utilities are used to sense and monitor owner's positions, movements, required signs, valuable usage, temperature as well as humidity levels of rooms along with sensing, controlling and monitoring capabilities, sensors cooperate and communicate with each other's to deliver, share and process sensed information and help real time decision making procedure through activate suitable alerts and actions. With such a rapid advancement, IoT applications are going to generate tremendous amount of data. The question is how to manage such a huge data. Traditional relational database have supported the storage and managing of data upto date but as the data generated by IoT devices does not have any semantics, RDBMS fails to handle it. Whereas NoSQL database claim to be more suitable and efficient for IoT as they are non-relational, schema free, horizontally scalable, easy replication support, etc. Also, ensuring privacy and providing enough security in the required services provided by IOTs is a major issue.

In this paper, we begin with general background of IoT, its requirements, databases and security concerns for IoT data. We have a discussion about which database is more suitable for IoT applications. The paper illustrates about IoT database requirements. The paper also performs a comparison study between SQL and NoSQL database technologies. The paper gives a brief on general information of security background of Internet Of Things and continue on with information security related challenges that Internet of Things will encountered. Lastly, we will also point out research directions that could be the future work for the solutions to the security challenges that IoT encounters.

KEYWORDS: Internet of Things (IoT), Database, SQL, NoSQL, information security, identification, sensing, authenticity.

I. INTRODUCTION

The Internet of Things (IoT) is a continuous emerging technology due to advent of internet [1]. It is associated with the objects, sensors and anything which is connected to the network and the internet and is able to communicate. [1] Internet of Things application ranges from smart cities to home automation to every other facet of our lives. IoT hence can be considered as a network of physical things where these physical things communicate and cooperate to share information with each other [7].

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 3, March 2017

When the term "Internet of Things" (IoT) was firstly introduced, the first question could be what is considered as "Things". Till recent years, groups of researchers and organizations tried to clarify the definition of IoT. The proposed definition of IoT with [10]" *A world where material objects are seamlessly integrated into a network of information , and where the physical objects can become active participants in business process.*" To extend the coverage of IoT definition, [11] it defines the "Things" from physical objects to virtual objects which represents as the identities with Internet connectivity. We can say IOT as [13] "Physical objects connected to physical objects in the internet"

Such type of Internet of Things applications generates a modest-sized data which needs to be stored for future analysis. The data needs to be kept in database. The significance of Internet of things (IoT) is not only that the more and more devices, systems, objects are getting connected to the internet but also that the data generated by an IoT environment is stored, processed, analyzed and are used for applying new and innovative analysis techniques for information gathering [4].

It is the proof that in future the application based on IoT will generate big data and this data will be analyzed further to make optimum use of resources. The use of IoT based applications will also result in real-time data generation which will make storing, accessing and processing data difficult [3]. The role of relational database management systems will persist while processing the data generated from vast number of enterprise IT systems is structured and has highly uniform data sets, where this data is managed in isolated manner. But when the data generated by millions and millions of sensors, devices and gateways is heterogeneous in nature the databases will require higher levels of flexibility, agility and scalability. So managing such big, unstructured or semi-structured data NoSQL databases have proven their value. NoSQL store data in a schema-free structure which helps in distributing the data with high scalability and availability. NoSQL databases have a capacity of 50000 inserts per seconds as compared to RDBMS which has only 5000 inserts per second. These properties are actually needed to realize the vision behind Internet of Things data. [1]

An increment phenomenon of user privacy data leakage and security vulnerability should not be overlooked in the IOT environment. A no. of significant research needs including security and privacy for future IOT system.
To establish the service infrastructure that provides security features. It is necessary to define the appropriate security features required for each component that make up the service infrastructure. For example: Data (User's privacy data) security is essential to the intelligent transportation service and intelligent medical services while authentication scheme is more important in the case of smart city and intelligent farm services.

Along with the growth of Internet of Things, new security issues and challenges arise while traditional security issues become more severe. The main and important reasons are the heterogeneity and the large scale of the objects. The factors which impacts can be further divided into two categories: the diversity of the "Things" and communication of that "Things". Now, it is divided mainly into two parts given that each of the categories encounters different security problems and causes.

First, the security problem for the "Things" is created by vulnerabilities which are produced by careless program design; this thing creates possibilities for malwares or backdoors installation. On the basis of heterogeneity and the scale of the "Things" in IoT, this type of security problems are more typical or complex in comparison of the security problems or issues that we have faced now.

The Internet of Things (IoT) opens opportunities for wearable devices, home appliances, and software to share and communicate information on the Internet. Given that the data which is shared contains a large amount of private information, preserving information security on that data is an important issue that cannot be neglected. The connecting of physical units, like thermostats, medical equipment and self-driving vehicles, to the Internet is happening very quickly and will most likely continue to increase exponentially for some time to come.

There have been many famous and technical publications by those in the software engineering, cyber security and systems protection describing issues and proposing various "fixes." Normally we can say that they address the "what"

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 3, March 2017

and the "why" of Internet of Things security, safety (protection) and privacy (with integrity), but not the "how."

There are many cultural, economic and other reasons why security, safety and privacy concerns are relegated to lower priorities. Also, when many systems are interconnected to each other, the overall security, safety or protection and privacy of the resulting systems of systems generally have not been totally considered and addressed. We will examine or analyse the costs of implementing suitable security, safety and privacy and the economic consequences of failing to do so.

As we know that for the communication medium of the "Things" (physical objects), it is expected that the networking environment for Internet of Things will be heterogeneous. Various types of communication media may face different security challenges. Overlooking these security and safety problems will compromise the availability of the "Things". And as for the contents of the communication, the heterogeneous data structure and protocols also make content protection more complex and complicated.

II. RELATED WORK

Authors [1] describes the various aspects of Internet of Things (IoT). It covers the definition of IoT, its different applications, issues related with Internet of Things, security concerns, privacy aspects as well as data generated by IoT devices. It specifies how the data generated is different in various aspects and the difficulties in co-relating it.

Authors [2] gives a brief understanding to the world of IoT. It states how the internet of things will connect the world in a smart fashion and will ease the business and human life. It specifies the three C's of IoT: Communication, Control and automation and Cost savings. The researcher gives an approach to reap the benefits of IoT into business if it addresses the sensors requirement, builds an IoT network and security foundation, collect indefinite amount of data and according to the size scale the IoT applications.

Authors [3,6] describes how the data generated by Internet of Things is huge and is going to be tremendous in the coming future. It specifies that the data generated by IoT is huge, unstructured and non-static. This data cannot be properly handled by Relational database management systems (RDBMS). As RDBMS cannot be fruitful for non-static schema, a new class of database has emerged, known as NoSQL. NoSQL database can easily handle and process the static-schema free structure which can be easily distributed providing scalability and high availability.

Comparative study [3] between NoSQL and SQL database is done with structured and unstructured data. In this work, author concludes that it is difficult to state which database system is superior without knowing the specific application of data definition and data querying. NoSQL database states that they prove to be better for heterogeneous data as compared to traditional SQL. The paper arises a question that which database to be used, the new and advanced NoSQL or more reliable traditional SQL.

NoSQL database is more efficient for IoT applications as compared to traditional database are specified in [4]. Platforms that manage the data needs to be more flexible, agile and should scale as required. Database should handle the dynamic and real time data. Also this data needs to be analyzed in certain applications of IoT such as healthcare where the data can be big data. Storing and processing such a data becomes easy with NoSQL.

Author [5] covers database requirements for IoT environment as well as different types of database used for IoT applications and also the benefits of various databases as per the application requirement.

Comparison of various database systems SQL & NoSQL [6] is done for moderate size data. It gives insight of runtime comparison for the database operations performed on the data. MongoDB does not require database schema or tables. MongoDB generates primary key for uniquely identifying each document. The results show the performance measures of NoSQL MongoDB and SQL RDBMS.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 3, March 2017

Authors [7] enlighten on the aspects of security and authorization of the data produced by IoT application.

[8] Data generated by IoT applications are huge, unstructured and so has an impact on storage which also makes data processing difficult with traditional database and so NoSQL is required. Requirements of the database storage system and ease of access gives rise to the use of NoSQL databases such as MongoDB, Cassandra, etc. To uniquely identify the devices for where the data is generated and the various protocols used for data transmission is also covered.

[9] Authors insights the need of IoT database storage on a local computer rather than creating a cloud. It builds up a database server on raspberry pi as it small and inexpensive and low-power consumption. It compares SQL with NoSQL and builds up the database using NoSQL MongoDB. It also states the advantages of using MongoDB over traditional RDBMS

Ensuring adequate security in IOTs is an ongoing challenge because of the sensors' severe resource boundaries and their demanding deployment environments based on applications. The unique properties of IOTs present a large number of valuable trades-offs in terms of the sensor's energy consumption and maintaining sufficient security measures. [10] We need to analyze and determine the exact security requirements of the home environment considering its distinctive properties, which are different from the environments and safety as well as security needs of a military battle-field, manufacturing shop floors, shopping centers or malls. At the basic level, considering the physical safety as well as security of the networks and their respective components, some research efforts should be driven to figure out preventive or protective measures to make the nodes tamper proof without much any overhead.

And the other important issue is to consider the robustness and resilience of Internet Of Things which are concerned with the strength of the network to provide an acceptable level of security if some nodes are compromised and the ability of the network to operate despite attacks. [11] Efficient mechanisms should be sought to quickly determine whether certain nodes are compromised and if so, they should be recognized and taken care of without affecting the normal functioning of the network. [13] Secure routing protocols, in general, provide little or no security features as well as properties and are susceptible to many types of attacks that results target routing disruption. Existing secure routing protocols in traditional networks can be investigated to see whether they can fit to WSNs. [12] Care should be taken to prevent adversaries from knowing about topology of the network. Accepting multi-path routing only when the regular routing path is corrupted by the presence of compromised nodes is a good way to circumvent malicious nodes, otherwise frequent and unnecessary dependence on multi-path routing can affect the energy consumption of the sensors.

III. THE INTERNET OF THINGS (IOT)

The initial evolution of the IoT was facilitated by advances in communications technology, greater network capacity, an expansion in the number of IP (Internet protocol) addresses, the proliferation of mobile devices, and growing acceptance of managing remotely.

The Internet of Things (IoT) is a network of globally identifiable physical things (or objects), their integration with the Internet, and their representation in the virtual or digital world. The IoTs allow people and things to be connected anytime, anyplace, with anything and anyone, ideally using any path/network and any service. The Internet of Things (IoT) is a system of interrelated computing devices, mechanical and digital machines, objects, animals or people that are provided with unique identifiers and the ability to transfer data over a network without requiring human-to-human or human-to-computer interaction.

[2] The Internet of Things (IoT) will connect both inanimate and living things, use sensors for data collection, will change what type of data will be communicated over IP. IoT data differs from traditional computing in many ways such as data generated by IoT applications can be very variable in size, the number of devices and nodes that are connected to the network in IoT are more in number, the frequency of data transmission, etc. Business will automate many if their functionalities due the machine-to-machine communication and intelligence that is offered by IoT applications. IoT

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 3, March 2017

technology offers to change the future of agriculture, industry, energy production and distribution of increasing available information [1]. Due to the IoT, ordinary things become smart and connected making it possible to access remote sensor data and to control the physical world from a distance.

[2] IoT has impact on every business. IoT will help business improve operations, gain efficiency, harness intelligence, improve and increase customer satisfaction. IoT will also have its impact on human's life. It will improve public safety, healthcare and transportation with better and faster communication of information. The three major benefits of IOT that will impact every business are: communication, control and cost savings. IoT promises to mark a start in a revolutionary, fully interconnected "smart" world, with defining objects, the relationships between objects and their environment and people and objects becoming more tightly intertwined.

It is clear from the definitions that IoT will produce a huge amount of unstructured data and IoT uses have intensified the need for privacy and safety, and particularly for security, well beyond current capabilities of both devices and infrastructures.

Costigan [12] lists some unintended consequences, as follows:

1. Further loss of privacy
2. Unforeseen disparities among groups and nations
3. Pre-crime forecasting
4. Unforeseen spillover across infrastructures
5. Economic disruption as IoT takes over certain jobs
6. Loss of ability to maintain understanding and control
7. New targets due to merging of virtual and physical

We must include many of these unintended consequences in our consideration of enforcing security, safety and privacy.

Pros and Cons of the Internet of Things

The Pros of IoT

1. Information: According to our opinion, it is clear that having more information helps us to making better decisions. [14] Whether it is mundane decisions as needing to know what to buy at the grocery store or if your company has enough widgets and supplies, knowledge is more powerful and more knowledge is better enough.

2. Monitor: The secondary and most obvious advantage of Internet of Thing is monitoring. Knowing the exact quantity of supplies or the air quality in home, offices or other places, can further provide more and more information that could not have previously been collected easily. For a instance, just knowing that you are low or down on milk or printer ink could save you another trip to the store in the near future. Further, monitoring the expiration of products can and will improve safety and security.

3. Time: As it is hinted in the previous examples, the amount of time which is saved because of IoT could be quite large. And in today's modern and fast life, we all could use more time.

4. Money: According to my opinion, the biggest advantage of IoT is saving money as well as time. If the price of the tagging and monitoring equipment is less than the amount of money saved, then the IoT will be very widely adopted.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 3, March 2017

The Cons of Internet of Things

1. Compatibility: Now a day, there is no international standard of compatibility for the tagging and monitoring equipment. This disadvantage is the very easy to overcome. The manufacturing companies of this equipment or devices just need to agree to a standard, like Bluetooth, USB, etc. This is nothing new or innovative needed.

2. Complexity: As with all complicated systems, there are more opportunities of failure. With the IoT, failures could sky rocket. For a instance, let us say that both you and your spouse each get a message telling that your milk has out dated or expired, and both of you stop at a store on your way home, and you both purchase milk. As a result, you and your spouse have bought double the amount that you both need. Or maybe a bug in the software ends up automatically ordering a new ink cartridge for your printer each and every hour for a few days, or after each power failure, when you only need a single replacement of that.

3. Privacy/Security: With all of this IoT data being transmitted, the risk of losing privacy and integrity increases. For an instance, how well encrypted will the data be kept and transmitted with? Or Do you want your neighbors or employers to know what medications that you are taking or your financial situation?

4. Safety: Just imagine if a notorious hacker changes your prescription. Or if a store automatically ships you an equivalent product that you are allergic to, or a flavor that you do not like, or a product that is already out dated. As a result, safety or security is ultimately in the hands of the consumer to verify any and all automation.

IV. REQUIREMENTS OF IOT

The requirements of IoT fall under three categories and at least two of these should be satisfied by your applications database platform:

1. An IoT sensor may generate millions of data records that are complex and heterogeneous in nature, which requires storing, indexing and identification.
2. Extracting values from IoT applications generated data focuses on minimizing latency on data ingestion for online querying and analytics.
3. The database should be horizontally scalable for the temporal and vast amount of data generated.
4. The database should be able to handle the diversity of the data.

V. DATABASE AND IOT

The Internet is moving towards to become Internet of Things where everything and everyone will be connected that embeds some intelligence in itself and are able to communicate, transfer information, conducts events and trigger actions. But the most important aspect of IoT is its database which collects and stores the ubiquitous data generated by sensing devices [9]. A database management system helps to handle the data, transfer the data, process the data and cover the different aspects of the data [1].

Database has basic characteristics which are given by CAP theorem that explains Consistency, Availability and Partitioning.

1. Consistency: It means after every update to the database, the latest version of it should be read by all its stakeholders.
2. Availability: It means that continuous operations can be performed on the database systems, which can be achieved by deploying database as cluster of nodes, replicating the data, etc.
3. Partitioning: It states that the database system should be up and running even if there is a node failure, which can be achieved by redirecting all the queries made to the failed to the working node.

The traditional database i.e. SQL focuses on consistency characteristic and provide with ACID properties:

1. Atomicity: Any transaction performed should be completely successful or unsuccessful.
2. Consistency: While performing a transaction, if a failure occurs the system should revert back to its pervious state.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 3, March 2017

3. Isolation: All the transactions are performed in isolation without any interference of each other.
4. Durability: A logs is maintained for all the committed transactions which help to recover from abnormalities.

RDBMS focuses on consistency characteristic but certain IoT application demands for availability and partition tolerance for BASE properties: Basic Availability, Soft State, Eventual consistency are implemented instead for ACID properties [1].

IoT communicates information to systems and people as well the sensor's collected data for example; state of the health monitoring equipment from the systems that are useful for monitoring a patient's vital sign. This data is used for further analysis of the patients in healthcare industry. Also IoT has its application in transport industry to check whether the parcel has been delivered on time and to a correct address. This data is used for further improvement of the delivery time and parcel conditions [6]. Such data holds a privileged position for increasing a company's performance and revenue. Many companies will tend to adopt IoT to save money. Companies deploys sensors needs to maintain a track of the data collected as though the data collected by a single sensor is not huge but companies will collecting data from millions of sensors, which needs to be stored and managed as this data will answer the questions of the future business [6]. Data generated in the Internet of Things needs storage and management more flexible, agile and scalable [2]. The data generated by IoT sensors and devices is heterogeneous in nature. It is all about join operations and spatiotemporal relationships [3]. Real time query handling and analytics, extracting information from the collected data and handling its storage is an important task [3].

VI. SQL AND NOSQL DATABASE FOR IOT

The most commonly used database is relational database which uses SQL as its query language. The ACID properties which are supported by SQL database require certain amount of overhead [4]. In RDBMS the data is stored in forms of interrelated tables which follow a strict schema [1]. RDBMS is used to capture the semantics of the data. RDBMS stores structured data where objects of the database having same format, type and equal number of characteristics are grouped together. Data is arranged into rows and columns where each row is uniquely identified having columns as its characteristics [4].

SQL speeds up its operations by using indexing [1]. Relational databases are simple, structures and flexible and are mainly used in banking and financial industries. It helps in maintaining data integrity. Tables in RDBMS are normalized resulting in multiple table creation. Querying those tables requires processing, fetching, combining and collecting information based on primary key and foreign key across multiple tables, which uses join operation. This results in SQL to be slow comparatively [4]. Searching for a row based on its primary key becomes difficult. Normalization prevents database to scale horizontally [8]. RDBMS can easily scale up but the problem lies in scaling it down [3].

RDBMS stores highly structured data. RDBMS stores the data in predefined tables, which is created before inserting the data. It is required to specify the required number of columns and the data types for each, which helps to maintain consistency but is not flexible enough to handle the data that is generated by IoT [8].

NoSQL is an abbreviation of 'Not Only SQL', is designed to meet the requirements of handling unstructured data which does not require any strict schema to store the data [2]. It provides distributed data store that supports large scale data storage [1]. NoSQL database are becoming more prominent these days as large amount data is collected today which is complex and unstructured in nature. For example, web pages for a single search query, video footages of public camera, etc. [4]. Data handled by NoSQL can be semi-structured such that similar objects having different characteristics are grouped together [4]. NoSQL databases are open-source, horizontally scalable and highly flexible [3]. NoSQL databases do not have interlinked relationship tables. Hence, the data generated by IoT applications can be easily handled by NoSQL. NoSQL are gaining popularity due to scalability, ease of access and speed.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 3, March 2017

There are different types of NoSQL. The most commonly used NoSQL database is based on key value pairs. NoSQL can be broadly classified into the following categories:

1. Document Store: This type of database store the data in form of documents. Each document contains multiple fields with unique identification of the document. These databases are more convenient for handling data items with complex structure.
2. Key-value: This type of database uses a key to uniquely identify a data item and the value can be any data having no strict semantics and structure. There are no join operations and the operations are limited. It provides easy scalability and good performance.
3. Column-family stores: This type of database are also known as extensible record stores, column oriented stores and wide column stores. It has columns family database and data items are stored in column families. The column family is treated as row which can be identified by a unique row key and which contains many columns.
4. Graph databases: This type of is made up of nodes and edges. Nodes represent entities and edges correspond to relationship between them. Graph databases can also store relationships. Due to such an organization between the nodes and the edges, direct relationships between the nodes can be quickly found out.

Difference between SQL and NoSQL

	SQL	NoSQL
Model	Relational database system	Non-relational or distributed database system
Schema	Strict or predefined	Dynamic schema for unstructured data
Data Storage	Data is stored in tables having rows and columns	Data is stored in either key-value pair, documents, graphs or wide-columns
Scalability	Vertically scalable	Horizontally Scalable
Querying language	Structured query language	Queries focused on collection of objects
Consistency	Strong Consistency	Eventually Consistency
Supported data structured	Structured data	Semi-structured or unstructured
For complex queries	Good for complex queries	Don't have standard interfaces to perform complex queries.
Type of data storage	Not good for hierarchical data storage	Highly preferred for large data sets
Examples	MySql, Oracle, Sqlite, Postgres and MS-SQL	MongoDB, BigTable, Redis, RavenDb, Cassandra, Hbase, Neo4j and CouchDb

VII. SECURITY REQUIREMENTS OF IOT

In this section, the security requirement area will be briefly described for the aspects of IoT infrastructure, cryptography, software vulnerability, malware, and mobile devices.

Components constituting the smart system, such as smart home, are likely to be exposed highly to a variety of threats from inside or outside because most of them have internet connectivity.
To cope with the security threats such as malware infections, unauthorized user access, important information disclosure, we should apply the security functions accordingly to the component specific characteristics of a smart system.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 3, March 2017

VIII. SECURITY REQUIREMENTS OF FOR A SMART SYSTEM BASED ON IOT

Category	Security Requirements
Confidentiality	User's privacy data delivered during the devices inter-communication and the key information used for the encryption algorithm should be managed securely to prevent potential exposure to the outside.
	In case sending the data generated from the smart system's devices into another device, the transferring data should be converted into cipher text form.
	To prevent the replication and modification by an outsider, identification information of a smart system device such as smart home system device should manage securely.
	Smart system devices should provide a highly secure password setting function and periodic password change functionality.
Integrity	To maintain the reliability and safety of devices, unauthorized device or user access should not be allowed.
	Through the mutual authentication between devices constituting a smart service, reliable communication environment must be configured.
Availability	To respond to security threats such as cyber-attacks and hacking, external attack detection capabilities must be equipped.
	The security features for software update of smart system's device must be provided.
	Periodic status monitoring of a smart system's device and unnecessary remote access blocking should be provided. In addition, if abnormal operations are generated from devices, appropriate response and event history about abnormal behaviour should be accompanied.

IX. SECURITY FUNCTIONS FOR A SMART SYSTEM BASED ON IOT

A) Confidentiality: In case of data communication between devices as well as sending data to the outside, the transferring data should be converted into cipher text form. That is, the data confidentiality should be provided. Here we recommend using any encryption algorithm such as RSA algorithm while sending data to the outside.

B) Integrity: Low capacity smart system's devices example: tiny sensors and actuators etc. and a server can use the access control function and mutual authentication function provided by the gateway.

C) Availability: To defend cyber-attacks including hacking from the outside, the firmware integrity verification should be provided.

X. CONCLUSION

In this paper, we have put a light on Internet of Things (IoT), its database requirements and usage, suitable database for the data generated by IoT devices and the data security requirement for the generated data. We have understood the environment of IoT with the aspects of database requirements and data security. We have compared SQL to NoSQL in various aspects. While comparing SQL to NoSQL we found that NoSQL seem to provide better solution for IoT generated data. However, SQL will still have its important role in handling the data generated. We also made an attempt to provide a survey on the issues of privacy and security of IOT. We have discussed several security problems and privacy issues that are present in IOT. The main features that differentiate IoT security issues from the traditional

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 3, March 2017

ones are the heterogeneous and large- scale objects and networks. These two factors, heterogeneity and complexity, make IoT security much more difficult to deal with.

REFERENCES

[1]. Karen Rose, Scott Eldridge, Lyman Chapin, "The Internet of Things: An Overview", Internet Society (https://www.internetsociety.org/iot), May 2015
[2]. LOPEZ Research LLC, "An Introduction to the Internet of Things (IoT)", Part1. Of "The IoT Series", November 2013
[3]. Sharvari Rautmare, Dr. D. M. Bhalerao, "SQL & NoSQL Database Study for Internet of Things", in International Journal of Innovative Research in Science, Engineering and Technology, Vol. 5, Issue May 2016
[4]. Emil Berthelsen, "Why NoSQL databases are needed for the Internet of Things", in Machina Research - Research Note, April 2014
[5]. Shona M, "Database Management in Different IoT Applications", in International Journal of Computational Engineering Research (IJCER), Vol. 06, Issue May 2016
[6]. Parker, Z., Poe, S., & Vrbsky, S. V. (2013, April). Comparing nosql mongodb to an sql db. In *Proceedings of the 51st ACM Southeast Conference* (p. 5). ACM.
[7]. Bouij-Pasquier, Imane, et al. "SmartOrBAC security and privacy in the Internet of Things." *Computer Systems and Applications (AICCSA), 2015 IEEE/ACS 12th International Conference of*. IEEE, 2015.
[8]. Gogawale, Anand, et al. "Database-as-a-Service for IoT." *Computing for Sustainable Global Development (INDIACom), 2016 3rd International Conference on*. IEEE, 2016.
[9]. Paethong, Pornpat, Mikiko Sato, and Mitaro Namiki. "Low-power distributed NoSQL database for IoT middleware." *Student Project Conference (ICT-ISPC), 2016 Fifth ICT International*. IEEE, 2016.
[10]. S. Haller, S. Karnouskos, and C. Schroth, "The Internet of Things in an Enterprise Context," in *Future Internet – FIS 2008 Lecture Notes in Computer Science* Vol. 5468, pp 14-28, 2009.
[11]. A. C. Sarma and J. Girão, "Identities in the Future Internet of Things," in *Wireless Personal Communications 49.3*, pp. 353-363, 2009.
[12]. C.S. Costigen, "Cybersecurity, the Internet of things, and the role of government," *Diplomatic Courier*, November/December 2014.
[13]. S. W. a. L. Brandeis, "The right to privacy, Harvard Law," pp. vol. 4, pp. 193-220,1979.
[14]. J. Zaddach, L. Bruno, A. Francillon, and D.Balzarotti. "Avatar: A Framework to Support Dynamic Security Analysis of Embedded Systems' Firmwares," In *Network and Distributed System Security Symposium*, February 2014